Разработка политик информационной безопасности

254 стр. PDF 2016 г.

В методическом пособии последовательно изложены все основные идеи, методы и способы практического решения разработки, внедрения, и поддержки политик безопасности в различных российских государственных и коммерческих организациях и структурах.

Приведенный материал пособия в первую очередь может быть полезен следующим группам специалистов: руководителям служб автоматизации (CIO) и служб информационной безопасности (CISO), внутренним и внешним аудиторам, менеджерам высшего эшелона управления, администраторам безопасности, системным и сетевым администраторам, администраторам БД.

Раздел 1. Актуальность политик безопасности

Как правило, руководители отечественных предприятий рассматривают проблему защиты конфиденциальной информации преимущественно с технической точки зрения. При этом решение названной проблемы связывается с приобретением и настройкой соответствующих технических средств защиты информации. Насколько современные аппаратно-программные средства защиты информации эффективны и достигли своей зрелости?

1.1. Эволюция технологий безопасности

- Новые темы безопасности
- Эволюция сети Интернет
- Международные аспекты кибербезопасности

1.2. Современные задачи безопасности

- Концепция автоматизации безопасности
- Когнитивные платформы BI
- Доверенные LTE-сети
- Организация MSSP

1.3. Оценка зрелости технологий безопасности

Современный рынок средств защиты конфиденциальной информации можно условно разделить на две группы:

- средства защиты для госструктур;
- средства защиты для коммерческих компаний и организаций.

Задачи, методы, требования, характеристики средств защиты информации для каждой из групп, существенные отличия. Также в данном разделе:

- подготовка к сертификации BS ISO 27001 (BS 7799-2), ISO 20000, ISO 9001, BS 25999;
- устранение замечаний аудиторов;
- кому и что доверять;
- трудности внедрения политик безопасности;
- состав группы по созданию политик безопасности;
- основные требования к политикам безопасности и др.

1.4. Возможные постановки задач

Рассмотрены возможные постановки задач по разработке и внедрению политик безопасности в отечественных компаниях и государственных структурах на примере металлургической компании.

- Цель разработки Концепции информационной безопасности
- Разработка стратегии информационной безопасности
- Основные требования к составу работ
- Требования к документированию проекта
- Российская специфика разработки политик безопасности

1.5. Дополнительные инициативы предприятий

Анализ и методическое рассмотрение ошибок при разработке и реализации стратегии ИТ-безопасности, построение модели управления рисками ИТ-безопасности, подготовке системы управления ИБ (СУИБ) компании на сертификацию ISO 27001 и пр.

А. Разработка стратегии ИТ-безопасности компании (подробно по этапам)

Б. Разработка модели управления рисками ИТ-безопасности (подробно по этапам)

В. Подготовка системы управления информационной безопасностью к сертификации (подробно по этапам)

1.6. Роль CISO в реализации проектов

Квалификационные требования к директору службы ИБ компании, его роль и основные задачи.

- Функциональные обязанности CISO
- Какие знания востребованы CISO?

Раздел 2. Рекомендации стандартов безопасности

В последнее время в разных странах появилось новое поколение стандартов в области защиты информации, посвященных практическим вопросам управления информационной безопасностью в компаниях и организациях. Это, прежде всего, международные стандарты BS ISO/IEC 27001:2013 и BS ISO/IEC 27002:2013, ISO/IEC 15408, ISO/IEC TR 13335, германский стандарт BSI, стандарты NIST США серии 800, стандарты и библиотеки COBIT 5, ITIL V3, SOX, SAC, COSO, SAS 78/94 и некоторые другие, аналогичные им. Как появление новых стандартов отобразилось на развитии нормативной базы по защите конфиденциальной информации в России? Какие нормативные документы (политики, стандарты, процедуры) стали востребованы в отечественных компаниях?

2.1. Стандарты BS ISO/IEC 27001 и BS 27001

2.2. Международный стандарт ISO 15408

2.3. Германский стандарт BSI

2.4. Стандарт COBIT 5

2.5. Законодательный акт Сарбейнса–Оксли (SOX)

2.6. Общие рекомендации по созданию корпоративных документов безопасности

В главе в табличной форме обобщены материалы, изложенные в предыдущих главах данного раздела.

2.7. Возможные проблемы и пути их разрешения

Среди наиболее общих проблем разработки требуемых политик безопасности следует отметить:

- сложности с поиском шаблонов или примеров подходящих по содержанию политик безопасности;
- недостаток собственных ресурсов или времени на разработку политик безопасности;
- сложности с обновлением политик безопасности, особенно в территориально распределенных компаниях, где мониторинг соответствия версий политик безопасности на конечных местах зачастую не осуществляется;
- обучение, тестирование и аттестация знаний персонала по безопасности обходятся слишком дорого или не достигают поставленной цели;
- сложности с обучением пользователей требованиям политик безопасности, отслеживанием компетентности сотрудников, потребность в использовании учебных средств с web-интерфейсом для снижения издержек на поездки сотрудников в центральный офис для обучения и тестирования (аттестации);
- сложности с доведением политик безопасности до конечных пользователей.

Раздел 3. Лучшие практики политик безопасности

Лучшие практики (Best Practices) разработки нормативных документов по защите конфиденциальной информации в организациях и компаниях. Это, прежде всего, практики разработки политик, процедур, стандартов и руководств безопасности таких признанных технологических лидеров, как IBM, Oracle, Cisco Systems, Microsoft, Symantec, SANS и пр.

3.1. Подход компании IBM

По мнению IBM, разработка корпоративных руководящих документов в области безопасности должна начинаться с создания политики информационной безопасности компании. Считается, что разработка политики безопасности относится к стратегическим задачам TOP-менеджмента компании. Основные этапы разработки политики безопасности:

- определение информационных рисков компании и мер по предупреждению их возникновения;
- разработка политики безопасности, которая описывает меры защиты информационных активов, адекватных целям и задачам бизнеса;
- выработка планов действий в чрезвычайных ситуациях для уменьшения ущерба;
- оценка остаточных информационных рисков и принятие решения о дополнительных инвестициях в средства и меры безопасности;
- структура документов безопасности;
- пример стандарта безопасности.

3.2. Подход компании Oracle

Политика безопасности как необходимость эффективной организации режима информационной безопасности. Здесь под политикой безопасности понимается стратегический документ, в котором ожидания и требования руководства компании к организации режима информационной безопасности выражаются в определенных измеримых и контролируемых целях и задачах.

- Определение ролей и обязанностей
- Структура политики безопасности
- Основное назначение политики безопасности
- Связь со стандартами и процедурами безопасности
- Основные идеи политики безопасности
- Этапы разработки политики безопасности
- Пример шаблона политики безопасности
- Пример политики безопасности

3.3. Подход компании Cisco Systems

- Создание политик использования
- Проведение анализа рисков, матрица безопасности
- Определение состава и структуры группы сетевой безопасности
- Подтверждение изменений в системах безопасности
- Мониторинг сетевой безопасности
- Нарушения безопасности
- Восстановление работоспособности серверов
- Пересмотр политики безопасности
- Пример политики сетевой безопасности

3.4. Подход компании Microsoft

Обязанности групп Corporate Security Group и Operations and Technology Group, традиционные подходы к управлению рисками (четыре этапа), методология на стандарте ISO 27002:2012 (BS 7799). Пример политики безопасности.

3.5. Подход компании Symantec

По мнению Symantec, руководящие документы в области безопасности (политики, стандарты, процедуры и метрики безопасности) являются основой любой успешной программы обеспечения информационной безопасности компании. Основные этапы разработки политики безопасности, а также:

- рекомендуемый состав политики безопасности;
- что принимается во внимание;
- требования к стандартам;
- процедуры.

3.6. Подход института SANS (www.sans.org)

Организация SANS выработала свой подход в понимании понятия политики информационной безопасности и ее составляющих. В терминологии SANS, политика информационной безопасности – многоуровневый документированный план обеспечения информационной безопасности компании (верхний уровень – политики, средний уровень – стандарты и руководства, низший уровень – процедуры).

- Основные политики компании.
- Функциональные политики.
- Обязательные стандарты (базовые).
- Рекомендуемые руководства.
- Детализированные процедуры.
- Пример политики аудита безопасности.

Раздел 4. Пример разработки политик безопасности

Рассмотрены основные положения некоторых политик и правил безопасности на примере предприятия связи:

- характеристика инфраструктуры компании;
- правила использования интернет-сервисов;
- правила доступа в сеть компании;
- правила обеспечения физической безопасности;

- архитектура корпоративной системы защиты информации;
- зона подключения к Интернету;
- зона доступа к web-приложениям компании;
- зона выхода в Интернет;
- зона управления ресурсами сети компании;
- зона защищаемых данных компании;
- зона внутренней сети компании.

Приложение 1. Шаблоны политик безопасности

- Политика классификации информации
- Политика инвентаризации информационных ресурсов
- Политика управления рисками ИБ
- Политика управления ролями ИБ
- Политика управления доступом к информационным ресурсам
- Политика управления данными
- Политика организации рабочего места
- Политика организации дистанционной работы
- Политика безопасности электронного документооборота
- Политика криптографической защиты информации
- Политика защиты от вредоносных программ
- Политика безопасности электронной почты
- Политика использования Интернета
- Политика использования программного обеспечения
- Политика использования мобильных устройств обработки информации
- Политика ведения переговоров и использования средств связи
- Политика физической защиты информационных ресурсов
- Политика управления сетевой безопасностью
- Политика безопасной разработки и эксплуатации АС
- Политика безопасности при техническом обслуживании
- Политика мониторинга событий ИБ
- Политика аудита информационной безопасности
- Политика управления инцидентами ИБ
- Политика кадровой безопасности
- Политика безопасности при работе с третьими лицами

Стандарты информационной безопасности

- ГОСТ Р ИСО 22301–2014
- ГОСТ Р ИСО/МЭК 27001–2006
- ГОСТ Р ИСО/МЭК 27002–2012
- ISO/IEC 27001–2013